THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN RE: CANON U.S.A. DATA BREACH LITIGATION This Document Relates To: All Actions	Case No.: 1:20-cv-06239-AMD-SJB **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Michael Finnigan, Kenneth Buchbinder, Brian McCartney, Tyrone Villacis, Luis Pichardo, Andre Hamid, Amy Lynn Hamid, Woodrow Moss, and Diana Rouse ("Plaintiffs") bring this Consolidated Class Action Complaint against Canon U.S.A., Inc., Canon Solutions America, Inc., Canon Software America, Inc., Canon Information and Imaging Solutions, Inc., Canon Financial Services, Inc., Canon Medical Components U.S.A., Inc., Canon Information Technology Services, Inc., and NT-ware USA, Inc. (collectively, "Canon" or "Defendants"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information that Defendants required from their employees as a condition of employment, including without limitation, names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth (collectively, "personally identifiable information," "Private Information," or "PII"). Plaintiffs also allege Defendants failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly

situated current and former employees and their beneficiaries and dependents (collectively, "Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Defendants are a leading provider of consumer, business-to-business, and industrial digital imaging solutions to the United States and to Latin American and the Caribbean markets. Defendants' employees entrust Defendants with an extensive amount of their PII. Defendants retain this information on computer hardware—even after the employment relationship ends. Defendants assert that they understand the importance of protecting such information.

3. On or before August 4, 2020, Defendants learned that a breach of Defendants' computer network had occurred and that it involved ransomware (the "Data Breach").

4. Defendants determined that the Data Breach involved unauthorized activity on their network between July 20, 2020 and August 6, 2020, including unauthorized access to files on Defendants' servers. These servers contained files that in turn contained the PII of Defendants' current and former employees and their beneficiaries and dependents.

5. On or around August 6, 2020, Defendants circulated an internal alert to their employees disclosing the Data Breach.

6. More than three months later, in a "Notice of Data Breach," dated November 24, 2020, Defendants advised that they were informing current and former employees of Defendants from 2005 to 2020, and their beneficiaries and dependents, of the Data Breach.

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII exposed to "unauthorized activity" included names, Social Security numbers,

driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth.

8. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and electronic signatures.

9. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited several months to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

10. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

12. Plaintiffs and Class Members have suffered injury as a result of Defendants'

conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

13. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Michael Finnigan is a resident and citizen of Ohio. Plaintiff Finnigan is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Finnigan's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Finnigan would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain

adequate data security. Plaintiff Finnigan's Private Information was compromised and disclosed as a result of the Data Breach.

15. Plaintiff Kenneth Buchbinder is a resident and citizen of New York. Plaintiff Buchbinder is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Buchbinder's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Buchbinder would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff Buchbinder's Private Information was compromised and disclosed as a result of the Data Breach.

16. Plaintiff Brian McCartney is a resident and citizen of New York. Plaintiff McCartney is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff McCartney's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff McCartney would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff McCartney's Private Information was compromised and disclosed as a result of the Data Breach.

17. Plaintiff Tyrone Villacis is a resident and citizen of Florida. Plaintiff Villacis is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Villacis' Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Villacis would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff Villacis' Private Information was compromised and disclosed as a result of the Data Breach.

18. Plaintiff Louis Pichardo is a resident and citizen of Florida. Plaintiff Pichardo is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Pichardo's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Pichardo would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff Pichardo's Private Information was compromised and disclosed as a result of the Data Breach.

19. Plaintiff Andre Hamid is a resident and citizen of Colorado. Plaintiff Andre Hamid is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Andre Hamid's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Hamid would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff Andre Hamid's Private Information was compromised and disclosed as a result of the Data Breach.

20. Plaintiff Amy Lynn Hamid is a resident and citizen of Colorado. Plaintiff Amy Lynn Hamid is acting on her own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Amy Lynn Hamid's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Amy Lynn Hamid would not have entrusted her Private Information to Canon had she known that Canon would fail to maintain adequate data security. Plaintiff Amy Lynn Hamid's Private Information was compromised and disclosed as a result of the Data Breach.

21. Plaintiff Woodrow Moss is a resident and citizen of New York. Plaintiff Moss is acting on his own behalf and on behalf of others similarly situated. Canon obtained and continues

to maintain Plaintiff Moss's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Moss would not have entrusted his Private Information to Canon had he known that Canon would fail to maintain adequate data security. Plaintiff Moss's Private Information was compromised and disclosed as a result of the Data Breach.

22. Plaintiff Diana Rouse is a resident and citizen of California. Plaintiff Rouse is acting on her own behalf and on behalf of others similarly situated. Canon obtained and continues to maintain Plaintiff Rouse's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Rouse would not have entrusted her Private Information to Canon had she known that Canon would fail to maintain adequate data security. Plaintiff Rouse's Private Information was compromised and disclosed as a result of the Data Breach.

23. Defendant Canon U.S.A., Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

24. Defendant Canon Solutions America, Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

25. Defendant Canon Software America, Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York, with its principal place of business in Melville, New York.

26. Defendant Canon Information and Imaging Solutions, Inc. is a corporation organized under the laws of New York, headquartered at One Canon Park, Melville, New York,

with its principal place of business in Melville, New York.

27. Defendant Canon Financial Services, Inc. is a corporation organized under the laws of New Jersey, headquartered at 158 Gaither Drive, Mt. Laurel, New Jersey, with its principal place of business in Mt. Laurel, New Jersey.

28. Defendant Canon Medical Components U.S.A., Inc. is a corporation organized under the laws of California, headquartered at 15955 Alton Parkway, Irvine, California, with its principal place of business in Irvine, California.

29. Defendant Canon Information Technology Services, Inc. is a corporation organized under the laws of Virginia, headquartered at 850 K Greenbrier Circle, Chesapeake, Virginia with its principal place of business in Chesapeake, Virginia.

30. Defendant NT-ware USA, Inc. is a corporation organized under the laws of Delaware, headquartered at 105 Maxess Road, Suite S129, Melville, New York, with its principal place of business in Melville, New York.

31. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

32. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

33. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

34. The Eastern District of New York has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in New York and this District through their headquarters, offices, parents, and affiliates.

35. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

36. Defendants are a leading provider of consumer, business-to-business, and industrial digital imaging solutions to the United States and to Latin America and the Caribbean markets with multiple subsidiaries, predecessors, and affiliates and more than 18,000 employees.

37. Plaintiffs and Class Members employed by Defendants were required to provide Defendants sensitive and confidential information for themselves and their beneficiaries and dependents, including names, dates of birth, Social Security numbers, electronic signatures, and other personally identifiable information, which is static, does not change, and can be used to commit myriad financial crimes.

38. Plaintiffs and Class Members, as current and former employees and their beneficiaries and dependents, relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand

security to safeguard their PII.

39. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

40. Beginning on or about November 24, 2020, Defendants sent Plaintiffs and other current and former employees and beneficiaries and dependents thereof a *Notice of Data Breach*. Defendants informed the recipients of the notice that:

> **What Happened?**
>
> We identified a security incident involving ransomware on August 4, 2020. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We also notified law enforcement and worked to support the investigation. We determined that there was unauthorized activity on our network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on our file servers.
>
> **What Information Was Involved?**
>
> We completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees from 2005 to 2020 and their beneficiaries and dependents. The information in the files included the individuals' names and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.[1]

41. On or about November 25, 2020, Defendants sent data breach notifications to various state Attorneys General, including California's Attorney General, signed by N. Scott

[1] Ex. 1 (Composite data breach notices filed with California Attorney General) at 10, available at https://oag.ca.gov/ecrime/databreach/reports/sb24-196551 (last visited Apr. 21, 2021).

Millar, Defendant Canon U.S.A., Inc.'s Senior Vice President & General Manager.[2]

42. Defendants admitted in the *Notice of Data Breach* and the letters to the Attorneys General that unauthorized third persons accessed files that contained sensitive information about Defendants' current and former employees and their beneficiaries and dependents, including names, Social Security numbers, driver's license numbers or government-issues identification numbers, financial accounts numbers provided to Defendants for direct deposit, electronic signatures, and dates of birth.

43. In response to the Data Breach, Defendants claim that they "immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We also notified law enforcement and worked to support the investigation…. We have already implemented additional security measures to further enhance the security of our network."[3] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again has not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

44. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

45. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class

---

[2] *Id.*

[3] *Id.* at 1, 5, 10.

Members, causing the exposure of PII for tens of thousands of current and former employees and their beneficiaries and dependents.

46. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

47. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full

[4] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Apr. 21, 2021).

office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

48. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to

[5] *Id.* at 3-4.

verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[6]

49. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

[6] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Apr. 21, 2021).

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[7]

50. Given that Defendants were storing the PII of tens of thousands of current and former employees and their beneficiaries and dependents, collected since at least 2005, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

51. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of current and former employees and their beneficiaries and dependents, including Plaintiffs and Class Members.

Defendants Acquire, Collect, and Store the PII of Plaintiffs and Class Members.

52. Defendants acquired, collected, and stored the PII of Plaintiffs and Class Members at least from 2005 to 2020.

53. As a condition of maintaining employment with Defendants, Defendants require that their employees entrust Defendants with highly confidential PII.

54. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were

[7] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Apr. 21, 2021).

responsible for protecting the PII from disclosure.

55. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

56. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially decade-old data from former employees and their beneficiaries and dependents.

57. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id.*

60. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

61. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

62. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Apr. 21, 2021).

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Apr. 21, 2021).

[12] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Apr. 21, 2021).

> calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

63. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

64. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

---

[13] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 21, 2021).

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Apr. 21, 2021).

black market."[15]

67. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

68. The fraudulent activity resulting from the Data Breach may not come to light for years.

69. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

70. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

71. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 21, 2021).

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Apr. 21, 2021).

72. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. To date, Defendants have offered Plaintiffs and Class Members only one year of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

74. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff Michael Finnigan's Experience

75. Plaintiff Finnigan was required to provide his Private Information to Canon in connection with his employment at Canon.

76. In or around November 2020, Plaintiff Finnigan received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Finnigan's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff Finnigan made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: accepting Canon's offer of credit monitoring; researching the Data Breach;

reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Canon; contacting his bank by telephone to inform them of the Data Breach. Plaintiff Finnigan has spent at least 2 hours dealing with the Data Breach, valuable time Plaintiff Finnigan otherwise would have spent on other activities, including but not limited to work and/or recreation.

78. As a result of the Data Breach, Plaintiff Finnigan has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Finnigan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

79. Plaintiff Finnigan suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Finnigan; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

80. Moreover, after the Data Breach, Plaintiff Finnigan also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages.

81. Plaintiff Finnigan has spent at least 2 hours since the Data Breach responding to these incidents as a result of the Data Breach. The time spent dealing with these incidents resulting

from the Data Breach is time Plaintiff Finnigan otherwise would have spent on other activities, such as work and/or recreation.

82. As a result of the Data Breach, Plaintiff Finnigan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Finnigan will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Kenneth Buchbinder's Experience

83. Plaintiff Buchbinder was required to provide his Private Information to Canon in connection with his employment at Canon.

84. In or around November 2020, Plaintiff Buchbinder received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Buchbinder's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

85. As a result of the Data Breach, Plaintiff Buchbinder made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Canon. Plaintiff Buchbinder now spends approximately 30 minutes per day reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 70 hours on these tasks,

valuable time Plaintiff Buchbinder otherwise would have spent on other activities, including but not limited to work and/or recreation.

86. As a result of the Data Breach, Plaintiff Buchbinder has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Buchbinder is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

87. Plaintiff Buchbinder suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Buchinder; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

88. Moreover, subsequent to the Data Breach, Plaintiff Buchbinder also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages which is an incredible volume. Plaintiff Buchbinder is borderline diabetic and does not take medication but since the Date Breach, he is receiving emails and letters in the mail from health companies that have his age and eligibility; emails and text messages related to mortgage debt; credit card date; fraudulent calls from IRS, FBI and Social Security.

89. Plaintiff Buchbinder has spent at least 20 hours since the Data Breach responding to these incidents as a result of the Data Breach. The time spent dealing with these incidents

resulting from the Data Breach is time Plaintiff Buchbinder otherwise would have spent on other activities, such as work and/or recreation.

90. As a result of the Data Breach, Plaintiff Buchbinder anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Buchbinder will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Brian McCartney's Experience

91. Plaintiff McCartney was required to provide his Private Information to Canon in connection with his employment at Canon.

92. In or around November 2020, Plaintiff McCartney received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff McCartney's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

93. As a result of the Data Breach, Plaintiff McCartney made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Canon as well as at least 4-5 phones calls to Canon regarding the Data Breach which totaled approximately 2.5 hours of his time. Plaintiff McCartney and his wife now spends approximately 20 minutes per day reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has

spent at least 182 hours on these tasks, valuable time Plaintiff McCartney otherwise would have spent on other activities, including but not limited to work and/or recreation.

94. As a result of the Data Breach, Plaintiff McCartney has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff McCartney is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

95. Plaintiff McCartney suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff McCartney; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

96. Moreover, after the Data Breach, Plaintiff McCartney also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. One email was from an anonymous person informing Plaintiff McCartney that they had his personal email and would release it if he did not pay them $10K in bitcoin.

97. As a result of the Data Breach, Plaintiff McCartney anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff McCartney will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Tyrone Villacis' Experience

98. Plaintiff Villacis was required to provide his Private Information to Canon in connection with his employment at Canon.

99. In or around November 2020, Plaintiff Villacis received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Villacis' Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

100. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching and enrolling in the credit monitoring and identity theft protection services offered by Canon. Plaintiff Villacis now spends time reviewing credit monitoring reports and/or checking account statements for irregularities, valuable time Plaintiff Villacis otherwise would have spent on other activities, including but not limited to work and/or recreation.

101. As a result of the Data Breach, Plaintiff Villacis has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Villacis is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

102. Plaintiff Villacis suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Villacis; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

103. Moreover, subsequent to the Data Breach, Plaintiff Villacis also experienced a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. The time Plaintiff Villacis spent dealing with these incidents resulting from the Data Breach is time Plaintiff Villacis otherwise would have spent on other activities, such as work and/or recreation.

104. As a result of the Data Breach, Plaintiff Villacis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Villacis will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Louis Pichardo's Experience

105. Plaintiff Pichardo was required to provide his Private Information to Canon in connection with his employment at Canon.

106. In or around November 2020, Plaintiff Pichardo received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Pichardo's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

107. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching and accepting credit monitoring and identity theft protection services offered by Canon. Plaintiff Pichardo now spends approximately 1 hour per month reviewing credit monitoring reports and/or checking account statements for irregularities. In addition, Plaintiff Pichardo changed his passwords on all his credit card accounts and bank accounts and opened a new bank account for his direct deposit as a result of the Data Breach. To date, Plaintiff has spent at least 15-20 hours on these tasks, valuable time Plaintiff Pichardo otherwise would have spent on other activities, including but not limited to work and/or recreation.

108. As a result of the Data Breach, Plaintiff Pichardo has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Pichardo is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. Plaintiff Pichardo suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Pichardo; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

110. Moreover, after the Data Breach, Plaintiff Pichardo also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages, causing him to change his phone number.

111. Plaintiff Pichardo has spent at least 15-20 hours since the Data Breach responding to these incidents and to mitigating damages as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Pichardo otherwise would have spent on other activities, such as work and/or recreation.

112. As a result of the Data Breach, Plaintiff Pichardo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Pichardo will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Andre Hamid's Experience

113. Plaintiff Andre Hamid was required to provide his Private Information to Canon in connection with his employment at Canon.

114. In or around November 2020, Plaintiff Andre Hamid received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Andre Hamid's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

115. As a result of the Data Breach, Plaintiff Andre Hamid made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including

but not limited to researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Canon, signing up and routinely monitoring the credit monitoring offered by Defendant. Plaintiff Andre Hamid now spends approximately 1 hour each month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 8 hours on these tasks, valuable time Plaintiff Andre Hamid otherwise would have spent on other activities, including but not limited to work and/or recreation.

116. As a result of the Data Breach, Plaintiff Andre Hamid has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Andre Hamid is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

117. Plaintiff Andre Hamid suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Hamid; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

118. Moreover, subsequent to the Data Breach, Plaintiff Andre Hamid also experienced actual identity theft and fraud, including a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages as a result of the Data Breach. Plaintiff Andre Hamid's email address was fraudulently used by an individual in Texas

to fill out a Wingstop customer satisfaction survey and Plaintiff Andre Hamid received emails from Wingstop in connection with this fraudulent activity.

119. Plaintiff Andre Hamid has spent at least 8 hours since the Data Breach responding to these incidents as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Andre Hamid otherwise would have spent on other activities, such as work and/or recreation.

120. As a result of the Data Breach, Plaintiff Andre Hamid anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Andre Hamid will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Amy Lynn Hamid's Experience

121. Plaintiff Amy Lynn Hamid's husband Plaintiff Andre Hamid was employed by Canon from May 2019 to June 2020 and provided Plaintiff Amy Lynn Hamid's Private Information to Canon for Ms. Hamid to receive health insurance and other benefits as Mr. Hamid's beneficiary.

122. In or around November 2020, Plaintiff Amy Lynn Hamid received notice from Canon that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Amy Lynn Hamid's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

123. As a result of the Data Breach, Plaintiff Amy Lynn Hamid made reasonable efforts

to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Canon, signing up and routinely monitoring the credit monitoring offered by Defendant. The time Plaintiff Amy Lynn Hamid has spent on these tasks is valuable time Plaintiff Amy Lynn Hamid otherwise would have spent on other activities, including but not limited to work and/or recreation.

124. As a result of the Data Breach, Plaintiff Amy Lynn Hamid has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Amy Lynn Hamid is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

125. Plaintiff Amy Lynn Hamid suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Canon obtained from Plaintiff Amy Lynn Hamid; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

126. As a result of the Data Breach, Plaintiff Amy Lynn Hamid anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Amy Lynn Hamid will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Woodrow Moss' Experience

127. Plaintiff Moss was required to provide his Private Information to Canon in connection with his employment at Canon.

128. In or around November 2020, Plaintiff Moss received notice from Canon that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Moss's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach.

129. As a result of the Data Breach, Plaintiff Moss made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; researching and accepting credit monitoring and identity theft protection services offered by Canon. Plaintiff Moss now spends approximately 1 hour per month reviewing credit monitoring reports and/or checking account statements for irregularities. In addition, Plaintiff Moss changed his passwords on all his credit card accounts and bank accounts and opened a new bank account for his direct deposit as a result of the Data Breach. To date, Plaintiff has spent at least 15-20 hours on these tasks, valuable time Plaintiff Moss otherwise would have spent on other activities, including but not limited to work and/or recreation.

130. As a result of the Data Breach, Plaintiff Moss has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling,

and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Moss is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

131. Plaintiff Moss suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Canon obtained from Plaintiff Moss; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

132. Moreover, after the Data Breach, Plaintiff Moss also experienced actual identity theft and fraud, including notification from CreditWise that his email address was compromised and found on the dark web. The email address found on the dark web is the same email he provided to Canon in connection with his employment at Canon. In addition, Plaintiff Moss received a Visa Debit card from Go2Bank in someone else's name with his address. Plaintiff Moss does not have an account at Go2Bank and does not know the person whose name is on the Debit card. Plaintiff Moss has also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages.

133. Plaintiff Moss has spent at least 15-20 hours since the Data Breach responding to these incidents and to mitigating damages as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Moss otherwise would have spent on other activities, such as work and/or recreation.

134. As a result of the Data Breach, Plaintiff Moss anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. As a result of the Data Breach, Plaintiff Moss will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Diana Rouse's Experience

135. Plaintiff Rouse was required to provide her Private Information to Canon in connection with her employment at Canon.

136. In or around November 2020, Plaintiff Rouse received notice from Canon that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Rouse's Private Information, including name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth, was compromised as a result of the Data Breach..

137. As a result of the Data Breach, Plaintiff Rouse made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching and purchasing identity theft protection for $24.99 per month from Experian; researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Rouse now and has since the Data Breach, spends approximately 4 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 25 hours on these tasks, valuable time Plaintiff Rouse otherwise would have spent on other activities, including but not limited to work and/or recreation.

138. As a result of the Data Breach, Plaintiff Rouse has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling,

and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Rouse is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

139. Plaintiff Rouse suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Canon obtained from Plaintiff Rouse; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

140. Moreover, subsequent to the Data Breach, Plaintiff Rouse also experienced actual identity theft and fraud, including monthly unauthorized charges of $10 per month since January 2021 for Uber Pass which she did not sign up for. In addition, Plaintiff Rouse has also been charged reoccurring Amazon Prime charges for $14.99 per month that she did not sign up for. Plaintiff Rouse has also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages. Since the Data Breach, Plaintiff Rouse is receiving between 5-10 spam phone calls from 5:00 a.m. to 10:00 p.m. every day that are very disruptive to her life as well as concerning. These fraudulent calls include threatening phone calls from the IRS that she owes money and if she does not pay, she will be arrested; calls from Apple and Microsoft saying that they need access to her laptop and from a Magistrate related to a case number and that someone will be coming to her home to arrest her. Plaintiff Rouse has received fraudulent emails from Chase Bank requesting confirmation of her bank account number. Plaintiff Rouse has blocked over 150 phone numbers.

141. Plaintiff Rouse spends at least 3 hours a week dealing with scam phone calls for a total of 72 hours since the Data Breach; spent at least 3 hours dealing with unauthorized charges

and expects to spend another 3 hours changing automatic billing instructions on her compromised credit and debit cards when she receives new cards. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Rouse otherwise would have spent on other activities, such as work and/or recreation.

142. As a result of the Data Breach, Plaintiff Rouse anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rouse will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

143. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

144. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Nationwide Class").

145. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Ross, and Rouse assert claims on behalf of a separate subclass, defined as follows:

> All current and former employees of any of Defendants residing in the United States who had contracts with any of Defendants related to PII that was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Employees Class").

146. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Amy Lynn Hamid asserts claims on behalf of a separate subclass,

defined as follows:

> All beneficiaries and dependents of any current or former employees of any of Defendants residing in the United States who had contracts with any of Defendants related to PII that was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Beneficiaries and Dependents Class").

147. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Buchbinder and McCartney assert claims on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in New York whose PII was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "New York Class").

148. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Finnigan and Moss assert claims on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in Ohio whose PII was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "Ohio Class").

149. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Rouse asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in California whose PII was compromised in the data breach first announced by Defendants on or about November 24, 2020 (the "California Class").

150. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Villacis and Pichardo assert claims on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in Florida whose PII was compromised in the data breach first announced by Defendants on or about

November 24, 2020 (the "Florida Class").

151. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

152. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

153. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendants have identified thousands of current and former employees, and beneficiaries and dependents thereof, whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records.

154. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class

Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

155. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to

Defendants' misfeasance.

156. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

157. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

158. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations,

like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

159. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

160. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

161. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

162. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Amended Complaint.

163. Further, Defendants have acted or refused to act on grounds generally applicable to

the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

164. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

165. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

166. As a condition of their employment with Defendants, Defendants' current and former employees were obligated to provide Defendants with certain PII, including their names, Social Security numbers, driver's license numbers or government-issued identification numbers, financial account numbers provided for direct deposit, electronic signatures, and dates of birth, and those of their beneficiaries and dependents.

167. Plaintiffs and the Nationwide Class entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

168. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

169. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

170. Defendants had a duty to exercise reasonable care in safeguarding, securing, and

protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

171. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

172. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

173. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendants with their confidential PII, a necessary part of employment with the company.

174. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

175. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

176. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

177. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

178. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

179. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

180. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

181. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

182. Defendants have admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

183. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendants' possession or control.

184. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

185. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

186. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former employees' PII, and that of their beneficiaries and dependents.

187. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove former employees' PII, and that of their beneficiaries and dependents, they were no longer required to retain pursuant to regulations.

188. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

189. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

190. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise

reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

191. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

192. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

193. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

194. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

195. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

196. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

197. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

198. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class)

199. Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

200. Defendants required Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class to provide their personal information, including names, addresses, Social Security numbers, driver's license numbers or government issued identification numbers, electronic signatures, dates of birth, financial information, the personal information of their beneficiaries and dependents, and other personal information, as a condition of their employment.

201. As a condition of their employment with Defendants, Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class provided their personal and financial information, including but not limited to the personal information of their beneficiaries and dependents. In so doing, Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class if their data had been breached and compromised or stolen.

202. Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class fully performed their obligations under the implied contracts with Defendants.

203. Defendants breached the implied contracts they made with Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class by failing to safeguard and protect their personal and financial information, including the personal information of their beneficiaries and dependents, and by failing to provide timely and accurate notice to them that personal and financial information, along with the personal information of their beneficiaries and dependents, was compromised as a result of the data breach.

204. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs Finnigan, Buchbinder, McCartney, Villacis, Pichardo, Andre Hamid, Moss, and Rouse and the Employees Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
THIRD-PARTY BENEFICIARY CLAIM
(On Behalf of Plaintiff Amy Lynn Hamid and the Beneficiaries and Dependents Class)

205. Plaintiff Amy Lynn Hamid and the Beneficiaries and Dependents Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

206. Defendants entered into agreements with their current and former employees related to PII that these current and former employees provided to Defendants, including PII of the current and former employees and their beneficiaries and dependents.

207. Defendants and their current and former employees formed an implied contract when these current and former employees provided PII to Defendants subject to this agreement.

208. Defendants current and former employees fully performed their obligations under the contract with Defendants.

209. The contract was intended for the benefit of the beneficiaries and dependents of Defendants' current and former employees whose PII was provided to Defendants.

210. The benefit to the beneficiaries and dependents of Defendants' current and former employees was clear and direct, not incidental, indicating that Defendants assumed a duty to compensate these beneficiaries and dependents if the benefit was lost.

211. The beneficiaries and dependents of Defendants' current and former employees lost the benefit of the contract because Defendants failed to protect their PII. Specifically, Defendants (1) failed to use reasonable measures to protect that information; and (2) disclosed that information to one or more unauthorized third parties, in violation of the agreement.

212. As a direct and proximate result of losing the benefit of the contract, the beneficiaries and dependents of Defendants' current and former employees sustained actual losses and damages as described in detail above, including but not limited to that they lost the benefit of the contract.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

213. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

214. Plaintiffs and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third

parties.

215. Defendants owed a duty to their current and former employees and their beneficiaries and dependents, including Plaintiffs and the Nationwide Class, to keep their PII contained as a part thereof, confidential.

216. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and the Nationwide Class.

217. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and the Nationwide Class, by way of Defendants' failure to protect the PII.

218. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

219. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their PII to Defendants as part of the current and former employees' employment with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

220. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiffs' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

221. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that their information security practices

were inadequate and insufficient.

222. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Nationwide Class.

223. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiffs and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiffs and the Nationwide Class to suffer damages.

224. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Nationwide Class in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Nationwide Class.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

225. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

226. At all times during Plaintiffs' and the Nationwide Class's interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's PII that Plaintiffs and the Nationwide Class employed by Defendants provided to Defendants.

227. As alleged herein and above, Defendants' relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiffs' and the Nationwide

Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

228. Plaintiffs and the Nationwide Class employed by Defendants provided Plaintiffs' and the Nationwide Class's PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized third parties.

229. Plaintiffs and the Nationwide Class employed by Defendants also provided Plaintiffs' and the Nationwide Class's PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

230. Defendants voluntarily received in confidence Plaintiffs' and the Nationwide Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

231. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Nationwide Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Nationwide Class's confidence, and without their express permission.

232. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

233. But for Defendants' disclosure of Plaintiffs' and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was

the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

234. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and the Nationwide Class's PII. Defendants knew or should have known their methods of accepting and securing Plaintiffs' and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Nationwide Class's PII.

235. As a direct and proximate result of Defendants' breach of their confidence with Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of current and former employees and their beneficiaries and dependents; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

236. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
VIOLATIONS OF THE NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiffs and the Nationwide Class, Or, Alternatively, Plaintiffs Buchbinder and McCartney and the New York Class)

237. Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs Buchbinder and McCartney and the New York Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

238. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Defendants misrepresented material facts to Plaintiffs and the Nationwide Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard the PII of Plaintiffs and the Nationwide Class from unauthorized disclosure, release, data breaches, and theft;

b. Defendants misrepresented material facts to Plaintiffs and the Nationwide Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of the PII of Plaintiffs and the Nationwide Class;

c. Defendants omitted, suppressed, and concealed material facts of the inadequacy of their privacy and security protections for the PII of Plaintiffs and the Nationwide Class;

d. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of the PII of Plaintiffs and the Nationwide Class, in

violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

e. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiffs and the Nationwide Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

239. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII that Plaintiffs and the Nationwide Class entrusted to Defendants, and that risk of a data breach or theft was highly likely.

240. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

241. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and the Nationwide Class) regarding the security of Defendants' network and aggregation of PII.

242. The representations upon which consumers (including Plaintiffs and the Nationwide Class) relied were material representations (e.g., as to Defendants' adequate protection of PII), and consumers (including Plaintiffs and the Nationwide Class) relied on those representations to their detriment.

243. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Nationwide Class have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

244. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, the PII of Plaintiffs and the Nationwide Class was disclosed to third parties without authorization, which has caused and will continue to cause damage to Plaintiffs and the Nationwide Class.

245. Plaintiffs and the Nationwide Class seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT VII
VIOLATIONS OF THE CONSUMER SALES PRACTICES ACT ("CSPA") OHIO. STAT. § 1345.02 ET SEQ. AND OHIO CONSUMER PROTECTION LAW §1349.19
(On Behalf of Plaintiffs Finnigan and Moss and the Ohio Class)

246. Plaintiffs Finnigan and Moss and the Ohio Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

247. CSPA prohibits an "unfair or deceptive act or practice in connection with a consumer transaction." Ohio. Stat.§ 1345.02(A).

248. In addition, CSPA also prohibits an "unconscionable act or practice in connection with a consumer transaction." Ohio. Stat.§ 1345.03(A).

249. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

250. While engaged in trade or commerce, Defendants have violated CSPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the personal and financial information of Defendants'

current and former employees and their beneficiaries and dependents from unauthorized access and disclosure; and

b. Failing to disclose that their computer systems and data security practices were inadequate to safeguard and protect the personal and financial information of Defendants' current and former employees and their beneficiaries and dependents from being compromised, stolen, lost, or misused.

251. Defendants failed to disclose the Data Breach to Plaintiffs Finnigan and Moss and the Ohio Class in a timely and accurate manner in violation of Ohio. Stat. § 1349.19(B)(2).

252. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII that Plaintiffs Finnigan and Moss and the Ohio Class entrusted to Defendants, and that risk of a data breach or theft was highly likely.

253. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

254. Defendants' failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs Finnigan and Moss and the Ohio Class) regarding the security of Defendants' network and aggregation of personal and financial information.

255. The representations upon which impacted individuals (including Plaintiffs Finnigan and Moss and the Ohio Class) relied were material representations (e.g., as to Defendants' adequate protection of personal and financial information), and consumers (including Plaintiffs Finnigan and Moss and the Ohio Class) relied on those representations to their detriment.

256. Defendants' actions constitute unconscionable or deceptive acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and

unscrupulous activities that are and were substantially injurious to Defendants' current and former employees, as well as their beneficiaries and dependents.

257. In committing the acts alleged above, Defendants engaged in unconscionable or deceptive acts and practices by omitting, failing to disclose, or inadequately disclosing to Defendants' current and former employees that they did not follow industry best practices for the collection, use, and storage of personal and financial information.

258. As a direct and proximate result of Defendants' conduct, Plaintiffs Finnigan and Moss and the Ohio Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

259. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, the PII of Plaintiffs Finnigan and Moss and the Ohio Class was disclosed to third parties without authorization, which caused causing and will continue to cause damage to Plaintiffs Finnigan and Moss and the Ohio Class. Accordingly, Plaintiffs Finnigan and Moss and the Ohio Class are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT VIII
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200, *et seq.* – UNLAWUL BUSINESS PRACTICES AND DECEPTIVE BUSINESS PRACTICES ACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Plaintiff Rouse and the California Class)

260. Plaintiffs and the Nationwide Class, or, alternatively, Plaintiff Rouse and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

261. Defendants' business practices as complained of herein violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL").

262. In violation of the UCL, Defendants have engaged in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200.

263. Specifically, Defendants engaged in unlawful acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting and gathering the PII of Plaintiffs and the Nationwide Class knowing that the information would not be adequately protected, and by storing the PII of Plaintiffs and the Nationwide Class in an unsecure electronic system in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to undertake reasonable measures to safeguard the PII of Plaintiffs and the Nationwide Class.

264. Defendants' actions and practices are "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiffs and the Nationwide Class outweighs the utility of Defendants' conduct. This conduct includes Defendants' failure to adequately ensure the privacy, confidentiality, and security of the PII that Plaintiffs and the Nationwide Class entrusted to Defendants and Defendants' failure to have adequate data security measures in place.

265. In addition, Defendants engaged in unlawful acts and practices by failing to timely and accurately disclose the data breach to Plaintiffs and the Nationwide Class, in violation of the duties imposed by Cal. Civ. Code § 1798.82.

266. Defendants knew or should have known that their data security practices with respect to their computer systems were inadequate to safeguard the PII of Plaintiffs and the Nationwide Class and that, as a result, the risk of a data breach or theft was highly likely. Defendants' unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Nationwide Class.

267. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiffs and the Nationwide Class suffered injury in fact and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

268. In addition, Plaintiffs and the Nationwide Class have incurred and will continue to incur economic damages related to the Data Breach, including loss of time and money spent remedying the Data Breach, and the costs of credit monitoring, purchasing credit reports, and implementing credit freezes to prevent opening of unauthorized account, among others.

269. Accordingly, Plaintiffs and the Nationwide Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and the Nationwide Class of money or property that Defendants acquired by means of their unlawful and unfair business practices, disgorgement of all profits Defendants received as a result of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and injunctive or other equitable relief.

COUNT IX
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200, *et seq.* – UNFAIR BUSINESS PRACTICES
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiff Rouse and the California Class)

270. Plaintiffs and the Nationwide Class, or, alternatively, Plaintiff Rouse and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

271. Defendants' practices as complained of herein violate California's UCL.

272. Specifically, Defendants engaged in unfair acts and practices by failing to establish adequate security practices and procedures, by soliciting and collecting the PII of Plaintiffs and the Nationwide Class, knowing that the information would not be adequately protected, and by storing the PII in an unsecure electronic system. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or damaging to Plaintiffs and the Nationwide Class as they were likely to deceive them into believing their PII was securely stored when it was not.

273. Defendants' actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiffs and the Nationwide Class outweighs the utility of Defendants' conduct. This conduct includes Defendants' failure to adequately ensure the privacy, confidentiality, and security of the data Plaintiffs and the Nationwide Class entrusted to them and Defendants' failure to have adequate data security measures in place.

274. Specifically, Defendants engaged in unfair acts and practices by failing to take appropriate action following the data breach to mitigate the effects of the Data Breach, enact adequate privacy and security measures, and protect the PII of Plaintiffs and the Nationwide

Class from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and damaging to Plaintiffs and the Nationwide Class.

275. As a direct and proximate result of Defendants' unfair practices and acts, Plaintiffs and the Nationwide Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

276. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and the Nationwide Class and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the abovenamed unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Nationwide Class.

277. Accordingly, Plaintiffs and the Nationwide Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and the Nationwide Class of money or property that Defendants may have acquired by means of their unfair business practices, disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and injunctive or other equitable relief.

278. Plaintiffs and the Nationwide Class reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq.*

COUNT X
VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT
CAL. CIV. CODE § 1798.150
(On behalf of Plaintiff Rouse and the California Class)

279. Plaintiff Rouse and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

280. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Rouse's and the California Class's nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Rouse and the California Class.

281. As a direct and proximate result of Defendants' acts, Plaintiff Rouse's and the California Class's PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendants' computer systems and/or from the dark web, where hackers further disclosed the PII of Plaintiff Rouse and the California Class.

282. As a direct and proximate result of Defendants' acts, Plaintiff Rouse and the California Class were injured and lost money or property, including but not limited to the loss of the California Class's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

283. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Class's PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Rouse and the California Class.

284. Defendant are affiliated companies organized or operated for the profit or financial benefit of their shareholders. Defendants collected their employees PII as defined in Cal. Civ. Code § 1798.140.

285. At this time, Plaintiff Rouse and the California Class seek only actual pecuniary damages suffered as a result of Defendants' violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

286. On April 20, 2021, Plaintiff Rouse provided written notice to Defendants identifying the specific provisions of this title she alleges they have violated. If within 30 days of Plaintiff Rouse's written notice to Defendants they fail to "actually cure" their violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff Rouse will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. See Cal. Civ. Code § 1798.150(b).

COUNT XI
VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA") FLA. STAT. § 501.201 *ET SEQ.*
(On Behalf of Plaintiffs Villacis and Pichardo and the Florida Class)

287. Plaintiffs Villacis and Pichardo and the Florida Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 164.

288. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204.

289. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the ransomware attack and Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

290. While engaged in trade or commerce, Defendants have violated FDUTPA, including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the personal and financial information of Defendants' current and former employees and their beneficiaries and dependents from unauthorized access and disclosure;

b. Failing to disclose that their computer systems and data security practices were inadequate to safeguard and protect the personal and financial information of Defendants' current and former employees and their beneficiaries and dependents from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Data Breach to Defendants' current and former employees and their beneficiaries and dependents in a timely and accurate manner in violation of Fla. Stat. § 501.171.

291. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII that Plaintiffs Villacis and Pichardo and the Florida Class entrusted to Defendants, and that risk of a data breach or theft was highly likely.

292. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs Villacis and Pichardo's and the Florida Class's personal and financial information entrusted to Defendants, and that risk of a data breach or theft was highly likely.

293. Defendants' failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs Villacis and Pichardo and the Florida Class) regarding the security of Defendants' network and aggregation of personal and financial information.

294. The representations upon which impacted individuals (including Plaintiffs Villacis and Pichardo and the Florida Class) relied were material representations (e.g., as to Defendants' adequate protection of personal and financial information), and consumers (including Plaintiffs Villacis and Pichardo and the Florida Class) relied on those representations to their detriment.

295. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendants' current and former employees, as well as their beneficiaries and dependents.

296. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendants' current and former employees that they did not follow industry best practices for the collection, use, and storage of personal and financial information.

297. As a direct and proximate result of Defendants' conduct, Plaintiffs Villacis and Pichardo and the Florida Class have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

298. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, the personal and financial information of Plaintiffs Villacis and Pichardo and the Florida Class was disclosed to third parties without authorization, which has caused and will continue to cause damages to Plaintiffs Villacis and Pichardo and the Florida Class. Accordingly, Plaintiffs Villacis and Pichardo and the Florida Class are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Employees Class, the Beneficiaries and Dependents Class, the New York Class, the Ohio Class, the California Class, and the Florida Class as defined herein, and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised,

hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: April 22, 2021

Respectfully Submitted,

/s/ *John A. Yanchunis*

Gary S. Graifman
Melissa R. Emert
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Telephone: (845) 356-2570

Facsimile: (845) 356-4335
ggraifman@kgglaw.com
memert@kgglaw.com

Gary E. Mason
David K. Lietz
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

Amanda Peterson (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

M. Anderson Berry
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com

Lori G. Feldman
GEORGE GESTEN MCDONALD, PLLC

102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-justice.com
E-Service: eService@4-Justice.com

David J. George
Brittany L. Brown
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
E-Service: eService@4-Justice.com

**pro hac vice* pending
Attorneys for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of April, 2021, I caused the foregoing, to be served via the Court's CM/ECF system, which will automatically send notice of such filing to all attorneys of record.

/s/ John A. Yanchunis
John A. Yanchunis